Bank Governance Leadership Network
ViewPoints

15 November 2010

TAPESTRY NETWORKS, INC · WWW.TAPESTRYNETWORKS.COM · +1 781 290 2270

Strengthening the board-management dialogue on risk and strategy

> Boards of directors[1] were unable to exercise effective control over senior management and to challenge the measures and strategic guidelines that were submitted to them for approval … [Boards'] failure to identify, understand and ultimately control the risks to which their financial institutions were exposed is at the heart of the origins of the [financial] crisis. – European Commission, *Green Paper: Corporate governance in financial institutions and remuneration policies*[2]

A board leader summed up the views of many fellow directors on risk governance quite simply: *"The most interesting question is, how can the board identify the real risks the organisation is [taking], in a world where technologies, products and institutions are all getting more complex? How do we have a real dialogue about this with the management team?"*[3]

Between January and October 2010, Tapestry Networks and Ernst & Young undertook an extensive inquiry into banks' current risk governance practices and their goals for continued improvement. Our research included data collection and interviews with chief risk officers (CROs) and risk executives from 17 major global banks, as well as conversations with risk chairs and members of board risk committees,[4] leading regulators and subject matter experts. It also encompassed a series of peer discussion sessions, including one amongst CROs, several dinners for non-executive directors and the second Bank Directors Summit, which took place 30 September–1 October 2010.[5]

Our work identified four imperatives for bank boards and risk organisations:

1. **Linking risk appetite to strategy decisions and business activities** *(Page 2)*

   Every major bank has invested a significant amount of board and management time in more clearly articulating its risk appetite. In the absence of a commonly-accepted definition, directors are actively engaging with management to develop bank-specific approaches based on answers to fundamental questions about their firms' long-term direction, appropriate risk capacity and resiliency under stress. Ongoing challenges include difficult-to-quantify risks, such as operational and reputational risks, and the incorporation of risk appetite into management decision-making.

2. **Fostering robust two-way dialogue on risk between directors and management** *(Page 11)*

   Directors and management alike are eagerly seeking more substantive boardroom dialogue on risk matters. Boards are changing risk committee operating practices to incorporate more forward-

---

[1] In this document, "director" refers to non-executive, non-employee board members on a firm's unitary or supervisory board.

[2] European Commission, Green paper: corporate governance in financial institutions and remuneration policies, (Brussels: European Commission, 2010), page 6.

[3] This document reflects the network's use of a modified version of the Chatham House Rule whereby comments made during conversations with participants, in italics, are not attributed to individuals or organisations. A list of research participants can be found in Appendix 1, on page 25.

[4] In this document, "risk committee" refers to the primary board-level committee tasked with responsibility for risk oversight. In banks without a separate risk committee, this is typically the audit committee.

[5] Ernst & Young and Tapestry Networks, "Banking industry challenges through the eyes of the non-executive director," *ViewPoints*, 15 November 2010.

planning, more time for unstructured discussion (often by handling approval and review items more efficiently) and more voices in committee meetings. Regulators have also expressed interest in better risk dialogue between boards and management, though it is unclear how they will assess progress.

3. **Improving the board's level of understanding of the firm's risks** *(Page 15)*

   Much time has been spent on efforts to enable directors to *"do more than just consume [risk information] … They need to be able to develop a point of view,"* as one regulator put it. Reports are becoming increasingly reader friendly and action oriented, with key assumptions made more transparent. But reporting is only half the challenge. Banks have been experimenting with ways to ensure directors receive sufficient high-quality education on an ongoing basis and have been attempting to ensure that all board members, not just those on the risk committee, have sufficient knowledge of the bank's risks to actively challenge management.

4. **Ensuring progress on risk governance is sustainable** *(Page 21)*

   While everyone acknowledges the progress that has been made in risk governance, boards and regulators want to ensure it will be effective in boom times as well as in bad ones. Directors and CROs fear escalating regulatory demands may become a drain on the risk function. Banks cite several factors as critical to maintaining effective risk governance over time: strengthening the risk organisation even more, notably the CRO's senior team, investing sufficiently in risk data systems and infrastructure, and ensuring boards have access to a variety of external perspectives on risk.

1. Linking risk appetite to strategy decisions and business activities

Banks have always been in the business of pricing, holding and selling risk. The concept of risk appetite – "[the] measure of the amount of total risk [an institution] is willing to accept in pursuit of its business goals"[6] – is thus hardly a new one in the industry, but research participants point out that prior to the financial crisis, banks had a somewhat more inward-focused, technical and *"oblique"* view of risk appetite. A chief risk officer reflected that historically, *"we thought about risk appetite intuitively. We knew what we liked."* A risk chair commented, *"We always discussed [risk appetite], but only recently have we done so in a formal way."* One regulator observed, *"Banks had a mainly interior view [of risk appetite]: setting and monitoring limits around quarterly earnings losses. Occasionally they might have done some scenario analysis, but there was no probing deep into the tail."*

All that has changed now. In publications and speeches by senior leaders, international organisations such as the Basel Committee[7] and the Committee of European Bank Supervisors (CEBS)[8] and domestic regulators such as the UK's Financial Services Authority (FSA)[9] and the Canadian Office of the Superintendent of

---

[6] J. Chris Karow, "Discovering Risk Appetite," *Crosscurrents: The magazine for financial services executives,* no. 31 (Ernst & Young Global Limited, Fall 2007).

[7] Basel Committee on Banking Supervision, *Principles for Enhancing Corporate Governance* (Basel: Bank for International Settlements, 2010), pp 15–16, 29.

[8] Committee of European Banking Supervisors, *High level principles for risk management* (London: Committee of European Banking Supervisors, 2010), page 4.

[9] Sally Dewar, "Taking the FSA's corporate governance agenda forward," speech at the City Corporate Governance and Remuneration Summit, 30 March 2010.

Financial Institutions (OSFI)[10] have singled out risk appetite as an area requiring significant board attention and focus to ensure risk appetite statements are appropriately holistic and well integrated into the firm's culture and activities.

Research participants highlighted the following challenges:

- Upgrading the bank's definition of risk appetite
- Addressing the special challenges of operational and reputational risk appetite
- Building risk appetite into management decision-making

Upgrading the bank's definition of risk appetite

One director with whom we spoke acknowledged, *"People know risk appetite is important … but the industry is still falling short on how to think about it. We don't have a paradigm yet."* A CRO observed, *"I haven't seen a lot of practical literature [on risk appetite]. It's mostly theoretical."*

Given supervisory authorities' heightened expectations for risk oversight, board members and risk executives have been looking to them for greater clarity on its definition, but thus far regulators have declined to provide specifics for fear of being overly prescriptive. CEBS states, "Risk appetite and risk tolerance depend not only on intrinsic risk aversion, but also on the current financial situation of the institution and its strategic direction … Institutions express their risk appetite and risk tolerance in a variety of forms."[11] One regulator, when asked what a good risk appetite statement would look like, responded, *"Great question. We don't have a good answer."*

In the absence of a clear paradigm, banks are pushing ahead with their own definitions of risk appetite. Directors are actively engaging with management in this effort: one CRO described a process of multiple iterations between the management-level risk committee and the board risk committee to revise and refine the exact wording of the risk appetite statement, which was subsequently approved by the full board.

Research participants highlighted four salient questions boards and risk committees should consider as they work with management to develop a robust definition of risk appetite:

1. What type of bank do we want to be?
2. How much risk do we want to take?
3. How are we funding risk taking across businesses?
4. How could internal and market-driven stresses affect our risk profile?

---

[10] Ted Price, "Defining the New Agenda for Governance at Financial Institutions," remarks to the RiskMinds USA 2010 Risk Regulation Summit, Cambridge, MA, 10 May 2010.

[11] Committee of European Banking Supervisors, *High level principles for risk management*, page 3.

1. What type of bank do we want to be?

Several banks are incorporating overarching statements of the firm's strategic goals into their definitions of risk appetite: as one CRO put it, *"[The risk appetite statement] describes our brand and expectations."* This use of the firm's vision and strategy as a starting point for risk appetite was endorsed by the non-executive directors attending the second Bank Directors Summit. One director attending the summit asked, *"Is risk appetite or strategy the chicken or the egg? I have come around to the view that strategy is the role of the full board and risk appetite is the role of the risk committee … Risk appetite falls out of strategy; it should not become too powerful a driver of strategy."*

2. How much risk do we want to take?

Many participants shared the view of the risk chair who asked, *"Have we left out any important quantifiable metrics [in our risk appetite]? … We really don't know."* Across the banks we interviewed, the most commonly cited risk appetite components are listed in the box below.

Risk appetite components in use by banks

Most participants include:

- Maintaining a target credit rating
- Stress scenarios
- Economic capital levels
- Profitability and earnings criteria (e.g., volatility, stability, diversity)
- Target value at risk (VaR) or VaR limits
- Operational risk indicators
- Regulatory compliance indicators
- Liquidity and capital ratios

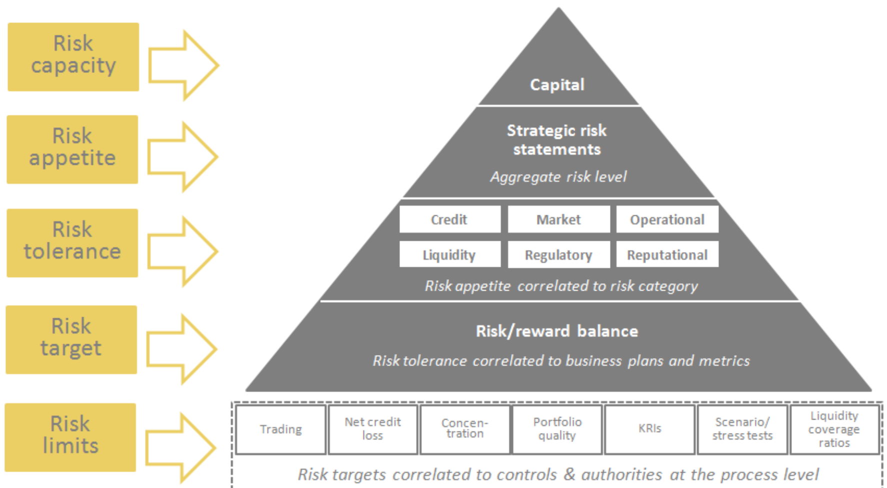
Several participants also cited:

- Loan loss ratios
- Asset quality and concentration
- Corporate reputation criteria (e.g., no business with specific sectors, countries)
- Market data indicators (e.g., share price, EPS, bond price, CDO spreads)

Several banks are incorporating relative comparisons to help inform risk appetite discussions between management and the board. According to one CRO, *"We decided we wanted our risk appetite to be lower than the average of our competitors."* Another bank takes into account the views of stakeholders when assessing risk appetite: *"[We ask], is our risk appetite outsized relative to the expectations of shareholders, or of regulators?"*

Participants emphasise that a firm's risk appetite should always be less than its capacity to take risk. As one director put it, *"The difference between risk capacity and risk appetite is that you can have food on the table, but you may still be on a diet."* A CRO agreed, *"By design, [business-level risk profiles are] less than* *risk appetite. It's designed to avoid hitting the limit for the whole enterprise."* Risk limits, in turn, are set within the boundaries of the risk appetite, and actual risk taking falls within risk limits.

The illustration below represents the relationships in pyramid form;[12] some risk executives use alternative approaches, such as concentric circles. Visual representations such as these can be helpful in communicating risk appetite and its implications throughout the company.



Directors and executives are well aware of the potential for board members to become so deeply involved in their institutions' risk-taking decisions that they end up overstepping the boundaries of their oversight role. Both groups note that boards need to be vigilant about not crossing the line. Regulators see the challenge as well: *"The more I think about it, the more I believe there is a real distinction between the limits the [risk] committee discusses with senior management and then the more granular limits that get translated down to the business level. The board can't be expected to know 1,000 limits … [They] don't need data at the trading-desk level."*

Individual boards and risk committees will continue working on calibrating the board's level of engagement on the implementation of risk appetite. While approaches will vary depending on each bank's structure and culture, industry participants highlighted the important role the risk limit structure itself can play in driving dialogue between management and the board. One head of risk said, *"Monthly, we review our tolerances against limits with the board. If we came close or exceeded something, [we ask] why? Was it a temporary issue? Was it due to the external environment?"* A former risk executive emphasised that the starting point for many boards must be a dialogue amongst directors themselves: *"In too many situations there is not agreement among board members about what happens when limits are broken … If someone breaks a limit and makes money, what happens? If they lose money, what happens? These are very interesting discussions."*

---

[12] Ernst & Young, Financial Services Office, 2010.

3. How are we funding risk taking across businesses?

A recent study by Ernst & Young and *CFO* magazine noted, "Capital management is the way that risk management finds expression in bank strategy at the highest level."[13] Boards and management have been devoting considerable attention and discipline to ensuring that strategy, risk and capital allocation decisions are made in concert. One research participant described how this plays out in the boardroom at his bank: *"If we approve X in the [business] plan, we need to take more risk. [We discuss] how that would flow through to our risk capacity and risk exposure … The board spends a good three to four hours in [this] discussion, and it is iterative over time, so in all, probably 10 to 12 hours."*

A director at a different bank noted the board is now looking closely *"at every business: what we did and how much capital it consumed. This allowed us to evaluate if we were using the right amount of capital for the expected returns. We also moved out of some businesses, once we focused on overall capital allocation."* A CRO commented, *"Our philosophy is whatever risk we take, we should be able to absorb it within the P&L [profit and loss] … We don't want to design our risk parameters such that if we have a situation slightly beyond the pale, we have to dip into our capital."*

Nearly all research participants said that the uncertainty over how future regulations will affect capital and liquidity requirements is significantly affecting strategy, risk appetite and capital planning discussions. Recently passed and emerging rules will establish higher capital thresholds, narrower definitions of tier 1 capital and increased requirements for capital adequacy across the economic cycle in order to address concerns about procyclicality.[14] Banks are already moving toward a more conservative approach to capital planning in anticipation of future regulatory standards: a chief risk officer with whom we spoke said, *"We moved from 10% to 12% to [even higher] tier 1 capital, and regulators still say we're not at a safe level."* Even some regulators acknowledge that, as one put it, *"We love capital; the more we can get, the happier we are … but [in the] long term, this could undermine the industry."*

4. How could internal and market-driven stresses affect our risk profile?

In the United States in April 2009, the Federal Reserve, Office of the Comptroller of the Currency and Federal Deposit Insurance Corporation conducted stress tests on 19 large global banks to assess expected losses and capital needs under two different macroeconomic downturn scenarios.[15] Fifteen months later, in July 2010, CEBS released results from a stress test exercise involving 91 European banks.[16]

---

[13] CFO Research Services and Ernst & Young, *Capital Management in Banking: Senior executives on capital, risk, and strategy* (Boston: CFO Publishing, 2010), page 4.

[14] See the Basel III consultative document, Basel Committee on Banking Supervision, *Strengthening the resilience of the banking sector* (Basel: Bank for International Settlements, 2010), and the G20 Seoul Summit Leaders' Declaration and Summit Document, 11–12 November 2010. See also Committee of European Banking Supervisors, *Implementation Guidelines regarding Instruments referred to in Article 57(a) of Directive 2006/48/EC recast* (London: Committee of European Banking Supervisors, 2010), and Ernst & Young, *Positioning for change: A roadmap for implementing US financial reform* (Ernst & Young Global Limited, 2010).

[15] Adrienne Carter, Mara Der Hovanesian and Ben Steverman, "The Fed Releases its Stress Test Scenario," *Bloomberg Businessweek,* 24 April 2009.

[16] Jack Ewing and Matthew Saltmarsh, "Doubts Persist as Most Europe Banks Pass Stress Tests," *New York Times*, 23 July 2010.

Bankers and commentators have raised various questions about the methodology and transparency of such supervisor-led efforts, as well as about the validity of scenario-based planning in general.[17] Meanwhile, banks themselves are conducting more stress tests and running more scenarios, often at the request of the board. One director commented, *"We are very actively discussing [stress scenarios] … What will happen to the business if we have a double-dip recession? What if the eurozone crisis deepens and some countries default or restructure? What will we do to mitigate the impact of these types of events, and what would the timing be?"* At the summit, a director described how a colleague on the risk committee handles overconfidence regarding the probability of major stress events: *"When anyone says, 'It will never happen,' he makes [management] run that scenario."*

To encourage a more comprehensive approach to stress testing, aimed at inducing banks to incorporate "sufficiently extreme macroeconomic outcomes" into their criteria, the FSA instituted a requirement in 2010 for banks to run so-called "reverse stress tests" that involve "explicitly identify[ing] and assess[ing] the scenarios most likely to render [their] business models unviable."[18] One regulator outside the UK stated, *"For my money, this is one of the best approaches boards can take. You start from the position of 'what could hurt us most' and go from there."*

Still, some regulators question whether bank boards are sufficiently engaged in reviewing and discussing the results of these exercises. One supervisor commented, *"We've found that a lot of the brainstorming and discussion on scenario planning is happening at the [executive] level … Are board members pushing management to see the extreme scenarios? One wonders how a set of scenarios which are designed and run by risk managers would be able to influence the board – or senior management in the businesses, for that matter."*

Addressing the special challenges of operational and reputational risk appetite

As directors and management continue to improve their firms' risk appetite definitions, they highlight operational and reputational risks as two types of risk that are particularly difficult to consider in the context of risk appetite. Directors are concerned that *"operational risk is still neglected."* One risk committee member reported, *"It comes up [at the board], but only when someone goofs."* At the summit, a director used overdraft charges as an example of an unseen reputational risk: *"No one thought about them, but they represented reputational and financial risk. How was that risk not identified in any [major] banks?"*

Regulators question banks' approaches to operational and reputational risk, characterised by one supervisor as *"'right-hand column of the* Wall Street Journal *risks' – the things that would make the board unhappy if published."* The Federal Reserve launched a horizontal review of compliance and other operational risks

---

[17] For commentary on regulators' stress tests, see Andrew MacAskill and Aaron Kirchfeld, "European Banks' Hidden Losses Threaten EU Stress Test," *Bloomberg Businessweek*, 6 July 2010. For a critique of scenario planning, see Lloyd Grove, "World According To … Nassim Nicholas Taleb," *Portfolio.com*, 14 August 2008, page 4.

[18] Financial Services Authority, "Reverse stress-testing," 4 August 2010.

earlier this year,[19] and CEBS recently released an updated consultation paper on operational risk management that included guidelines for internal controls and reporting mechanisms.[20]

Risk organisations are struggling to incorporate both the internal and external components of risk in these areas. Several CROs agreed with one who said, *"We haven't had any major breakthroughs. We're evolving our model for operational risk and don't yet have one for reputation risk."* In part, this is due to the broad definitions and qualitative nature of these risk categories, encompassing everything from fraud risk to worker health and safety issues in the case of operational risk, and from customer satisfaction data to *"finding the next Madoff in your client base"* in the case of reputational risk. As one risk executive observed, *"The relationship of some metrics to reputational risk [is unclear] – how scientific [can we really be]? … I am much more concerned about underwriting for a [bad] company in a [risky] part of the world."*

Reputational and operational risk indicators in use by banks

- Customer survey data
- Published indexes, e.g., corporate responsibility indices or "Most Admired" ratings
- Supervisory notices and alerts
- Red-flag issues with clients or vendors
- Reports on major pending or in-process projects, e.g., IT systems upgrades
- Unresolved items from internal or external audits
- Occupational health and safety incidents

Participants said that internally, with regard to limiting operational risks, *"we need to ensure there's no way to do [internal processes] other than the right way."* The bank must also monitor risks related to changes in personnel. One director stated, *"I think this is huge. So many people have been let go. We have lots of new employees, and there are still some vacancies … How does that affect risk?"* Externally, banks must maintain focus on *"market conduct [and] treating our customers fairly."* Many research participants mentioned new products in the context of market-conduct risk and urged boards to ask, *"What are they for, and to whom are we selling them?"*

While granting that risk appetite is still a *"work in progress,"* directors and risk executives are encouraged by their progress. The CRO who described his bank's pre-crisis approach to risk appetite as *"intuitive"* remarked, *"We knew what we liked. Now, we know very well what we don't like – this helps us to better understand what we do like, and also what is too much of a good thing."*

[19] Victoria Tozer-Pennington, "US Fed working on horizontal reviews of op risk issues," *Risk.net*, 30 March 2010.

[20] Committee of European Banking Supervisors, *Revised consultation paper on the management of operational risk in market-related activities* (London: Committee of European Banking Supervisors, 2010).

Building risk appetite into management decision-making

Risk committees, boards and management are actively working to incorporate risk appetite into key strategic decisions, including those regarding annual business planning and budgeting, evaluations of new products and business activities and assessment of remuneration[21] risk.

- **Annual business planning and budgeting.** A well-understood risk appetite helps ground business planning discussions: as one risk chair explained, *"If we decide to stop doing X, or de-risk in business Y, the business needs to know so they can plan for it."* Another director agreed: *"Staffing, resources, capital levels – they all have to add up to align with the [core risk appetite]."* One bank plans to update its risk appetite statement following the annual board strategy offsite and then will cascade it into annual operating plans at the business unit level. The CRO of another bank noted that risk appetite approval *"[was] purposely [done] ahead of our operating planning session … We worked through the risk appetite framework in late Q3, early Q4,"* prior to the board's sign-off on the strategic and operating plans later in the fourth quarter.
- **Evaluations of new products and business activities.** Board members agreed broadly with a director, who, speaking last year, said, *"[We directors] should be able to put up our hands and say, 'We are not getting into that business.'"* Using risk appetite as a litmus test for new products or businesses, or for proposed changes to existing activities, helps to *"root out strategic drift as early as possible – we stay disciplined."* Several participants described instances in which their banks decided to discontinue certain products, exit businesses or forgo entering new areas as a result of the firm's established risk appetite. Regulators strongly encourage banks to apply risk appetite as a filter for business and product decisions; indeed, the guidelines of several regulatory bodies, including CEBS,[22] follow the Walker Report's recommendation and say that the risk function should play an active role in such decisions and should even have a "veto where necessary."[23] At the board level, one regulator recommended that directors ask the following questions about business entry and exit activity: *"What are we doing with businesses not critical to our strategy? What are the implications for our portfolio – [will we be] more or less concentrated than we should be? Are the businesses we want to move into going to make our portfolio more or less volatile, on average?"*
- **Assessment of remuneration risks.** Banks have been working to implement the Financial Stability Board's (FSB's) principles for sound compensation practices,[24] which address alignment of pay structures with risk and the role of the board in remuneration governance. They are doing so whilst simultaneously keeping track of additional changes and requirements entailed by an ongoing stream of new regulation, including new restrictions on banker bonuses in Europe[25] and investor "say on pay"

---

[21] The terms "remuneration" and "compensation" are used interchangeably throughout this document.

[22] Committee of European Banking Supervisors, *High level principles for risk management,* pp 5–7.

[23] David Walker, *A review of corporate governance in UK banks and other financial industry entities* (London: HM Treasury, 2009), page 85.

[24] Financial Stability Board, *FSB Principles for Sound Compensation Practices* (Basel: Financial Stability Board, 2009), and *FSB Principles for Sound Compensation Practices: Implementation Standards* (Basel: Financial Stability Board, 2009).

[25] See "Europe hikes capital rules, slashes banker bonuses," *Risk.net*, 9 July 2010, and Financial Services Authority, "FSA consults on changes to its Remuneration Code," press release, 29 July 2010.

rules in the United States.[26] At the summit, directors acknowledged that *"it's [been] 'heads we win, tails you lose' for banks and banker compensation"* and agreed that *"deferral and clawback for anyone dealing with other people's money should apply."* However, research participants expressed concern that boards are being pushed toward a *"tick-the-box"* approach to assessing pay risk; others pointed out that the requirements are sometimes unreasonable: *"Regulators are all over us to do impractical things."*

Several research participants questioned whether much has really changed, despite the wave of new requirements. One subject matter expert with whom we spoke commented, *"There's a big difference between getting the profit pool [properly risk-adjusted] and simply making a guess and saying, 'We'll institute a clawback if we end up being wrong.' Most banks have done the latter, not the former."*

Risk-adjusting incentive pay

A specific challenge for many banks is determining how to risk-adjust bonus pools for executives and risk takers, an area that the FSB declared in 2010 had "significant room for improvement." [27] Challenges include:

- Identifying the individuals and teams with the potential to create the greatest impact on the firm's risk profile.
- Deciding which metrics to apply: the CROs with whom we spoke are experimenting with a variety of methods, including actual versus planned economic value added, volatility of the P&L statement and the liquidity level of securities.
- Covering all components of bonus pay, which one CRO described as *"a two-step process. First, we have to determine the size of the bonus pool adjusted for risk. Then, the deferred component of [variable pay] will also have to be adjusted for risk."*
- Establishing a workable steady-state role for the CRO: *"I've attended every compensation committee meeting for the past year,"* one CRO observed. This CRO continued, *"That may not necessarily be the model indefinitely … but it won't drop [back] to once a year."*

Directors and management need to ensure their institutions' risk appetite frameworks provide clear and consistent direction to guide business decisions and strategy setting, without becoming overly rigid and, ultimately, losing relevance. After all, as one chief risk officer observed, *"The idea of what's low or high risk is always changing – and it changes outside our [scheduled] planning period."* Most boards report that they plan to revisit the overall risk appetite statement and parameters on an annual, or in some cases a semi-annual, basis, given the shifting regulatory environment and expected changes to capital and liquidity requirements. The risk appetite statement will also change as firm strategy evolves. At one bank, *"while*

[26] Ernst & Young, *Positioning for change: A roadmap for implementing US financial reform,* page 3.
[27] Financial Stability Board, *Thematic Review on Compensation: Peer Review Report* (Basel: Financial Stability Board, 2010), page 9.

we're still aiming to be [conservative], we've added words this year about pursuing judicious business growth where there are market opportunities."

Questions for risk committees and CROs to consider:

- ? How have you defined the roles of the full board, of key committees and of management, respectively, in setting the institution's risk appetite?
- ? Does everyone at the firm share the same view of what is meant by risk appetite and its key components? How does the firm decide when risk appetite should change? What roles do the risk committee and the full board play in these decisions?
- ? What thresholds does the board use to determine when it should get involved in setting risk limits? What happens when limits are broken?
- ? How comfortable are you with the firm's ability to assess reputation and operational risks? Are there any risk areas you believe are not getting sufficient attention from management, and if so, what has been the board's response?
- ? What approaches for integrating risk appetite into the board's strategy and business planning discussions have proven most effective?

2. Fostering robust two-way dialogue on risk between directors and management

Directors take seriously the responsibility laid out by Sir David Walker to "ensure that there is open debate and challenge within both the executive team and the full board."[28] One challenge they face is balancing what seems like an ever-increasing set of policy approvals and other regulatory requirements with time for open discussion. A risk committee chair asked, *"How do [we] define the issues that are central to our work and allocate [our] time? Should we really be two-thirds compliance and one-third higher-level discussion, or the other way around?"* Boardroom culture is also an important determinant of the quality of dialogue. Another risk chair observed that *"[management] doesn't like to say what's important because they're afraid they'll miss something. We ask them to just tell us the story. Instead, they give us a bunch of data."* One CRO acknowledged that *"[management] tends to be very structured and focused. They want control, so they do a presentation, and then there's no discussion."*

Research participants described ways in which they are working to improve the dialogue between directors and management and how regulators are approaching the task of assessing the quality of that dialogue:

- Changing risk committee operating practices
- Working with the CRO
- Assessing the quality of risk dialogue

[28] David Walker, *A review of corporate governance in UK banks and other financial industry entities,* page 42.

Changing risk committee operating practices

Many of the risk chairs and committee members with whom we spoke commented that months after the height of the financial crisis, *"the volume of work is incredible"* and *"agendas are still heavy."* Fewer firms are managing with only quarterly risk committee meetings in today's environment: a majority of participants report six to eight "routine" (i.e., scheduled) risk committee meetings per year, with as many as 12 at the high end of the scale. Most last between two and three hours, though several committees' meetings run longer, in the range of four to five hours.

How are risk committees working with CROs to maximise the value and efficiency of all this time spent together? Participants highlighted a number of approaches to committee meeting design and operations that can create opportunities for richer dialogue between management and the board:

- **Engage in forward planning to define committee objectives for the year ahead.** The risk chair at one bank ensures that the committee *"produce[s] a list of five or six objectives for the year, things we're planning to achieve … [It helps identify] the discussions [we] absolutely want to have and how deeply we want to go."*
- **Find ways to cover required approval items more efficiently.** In order to address policy approvals and other compliance items in a thorough but expeditious manner, risk committees are using consent agendas or discussion by exception more frequently. One bank has added risk committee teleconference calls, scheduled between in-person meetings, to cover regulatory items. Participants noted that the committee chair plays a critical role in keeping discussion moving in a timely fashion, whether for routine items or other topics.
- **Set aside a generous portion of time for unstructured discussion.** Some risk committees prefer to start meetings with an "open discussion" agenda item, while others reserve time for it at the end of each session. Many participants agreed with the head of risk who described it as *"the most important part of the meeting."* One CRO commented, *"We reserve about an hour for roundtable dialogue and would like to make it even longer."* Setting aside time for unplanned discussion, with no standing agenda and no prepared presentations, helps to keep dialogue fresh: *"If the agenda stays roughly the same every time, [meetings] ultimately will get sterile."* Several participants emphasised that in order to be effective, these unstructured discussions need to be more substantive than a brief "current events" or "all other business" item.
- **Ensure a range of voices are represented.** Directors and risk executives emphasise that, ultimately, business leaders are accountable for risk. This accountability is demonstrated in the risk committee, according to most participants, by business unit representatives being present for relevant portions of the discussion: *"If [the CRO] is discussing X risk with the board, that business unit leader is in the meeting. It's a joint presentation."* One CRO described a process whereby *"the business leaders talk through their view on risks, and then they're asked to leave. Then the board asks me [to comment]."* A regulator with whom we spoke encouraged risk committees to actively involve the internal audit function in the risk dialogue as well: *"The risk function [can be considered] part of*

management. Internal audit is the eyes and ears of the board … Are directors asking internal audit to evaluate the firm's risk management capabilities?"

- **Provide guidance to management on how to interact with the committee.** Several directors with whom we spoke expressed frustration that committee discussions with management are limited by executives' *"presentation mentality."* A head of risk acknowledged, *"I've tried to tell my team to keep remarks brief, but they're not there yet. I've considered not allowing my team to [lead and just] hav[ing] them answer questions."* The IIA Research Foundation recommends that audit chairs provide explicit guidance to management on how to interact with directors in committee meetings; if necessary, the board should request that management send a different individual to discuss a particular topic with the committee.[29] Risk chairs may wish to consider adopting a similar approach.

Typical risk committee agenda items

Most risk committees regularly include:

- Review of risk appetite, limits
- Review of enterprise risk report
- Business unit risk reviews
- Reviews of specific risks by category
- Policy approvals
- Current events/trends and resulting impact on risk
- Treasury, audit updates

Several participants also cited:

- In-camera sessions (e.g., non-executive directors with CRO or auditor)
- Reviews of business continuity plans
- Benchmarking against peers
- Review and approval of transactions

Working with the CRO

Several participants said that high-quality, open dialogue between management and the risk committee requires an open communication channel between directors and the CRO. Participants cited private sessions between the CRO and risk committee (or risk chair alone) and collaboration between the CRO and the risk chair on meeting agenda development as good methods of encouraging an active dialogue. In one bank, the risk chair and CRO work through the meeting beforehand, then work together in the meeting to keep on time.

At one bank, the head of risk maintains an open-door policy to encourage committee members or any other non-executive directors to visit and discuss top-of-mind issues. One director stressed the importance of

[29] The Institute of Internal Auditors Research Foundation, *Audit Committee Effectiveness – What Works Best,* 3rd ed. (Altamonte Springs, FL: Institute of Internal Auditors Research Foundation, 2005), page 93.

reaching out to the CRO on an ongoing basis, to build a baseline of candid communication: *"I invest a lot of time with our risk director, and also the CFO, outside of meetings. Every time I meet with them, I make sure to ask, 'Is there anything else you want to tell me?' I never want to put them in a position of having to come and find me if something is wrong."*

Assessing the quality of risk dialogue

Regulators say they will be paying close attention to the evolution of board-management dialogue on risk. In its consultation paper on corporate governance principles published in early 2010, the FSA gave notice that it would be "looking for evidence of depth of understanding and effective discussion [and] challenge" in key areas, including risk discussions, emphasising an increased focus on the role of non-executive directors and especially on committee chairs.[30]

Some supervisors plan to use interviews with board members and executives to develop a view on the strength of board-management discussions on risk. One regulator observed, *"We don't want to sit in on committee meetings, because it will change the dialogue. We'll engage with board members by meeting with them three or four times a year."* Other regulators seem to have fewer reservations about the impact of their presence on committee discussions. One director reported receiving visits from both the Federal Reserve and FSA at recent risk committee sessions. Another director commented, *"[Regulators] are asking us if they can sit in on committee meetings. I don't think this is a time when we can say no."* Some regulators acknowledge the difficulty of evaluating the level of dialogue between the board and management, whatever their chosen approach: *"These are hard judgment calls to make,"* one said, while another noted that this assessment requires *"a fundamentally different skill set for examiners; it's not the same as technical competence with risk issues."*

While several risk chairs and committee members commented on regulators' efforts to assess the quality of risk dialogue, the issue of how risk committees themselves might formally evaluate progress did not come up. At a meeting of European audit committee chairs, participants shared some ways in which they evaluate committee effectiveness that may have relevance for risk committees. These include adding questions to the board-level assessment, conducting separate committee-specific evaluations, the periodic use of external consultants and seeking the opinion of the external audit firm.[31]

What changes do directors and management hope to bring about? In the words of one risk chair, *"The key is to get [management] to understand that questions don't represent a lack of confidence; [they] should be welcomed."* A chief risk officer expressed a similar view: *"It's a win-win feeling – you can really sense it when you have it. If the [conversation] is win-lose – 'I wanted a limit of $1 billion and you gave me $800 million, so I lost' – forget it."* Another CRO mentioned that while better dialogue is unlikely to make committee meetings shorter, meeting content will undoubtedly be richer as a result: *"We won't be spending*

---

[30] Financial Services Authority, *Effective corporate governance (Significant influence controlled functions and the Walker Review)* (London: Financial Services Authority, 2010), page 32.

[31] European Audit Committee Leadership Network, "Enhancing audit committee effectiveness in a changing environment," *ViewPoints*, 30 April 2010, pp 3–4.

less time with the committee [than before], but we'll have more informed discussion. Just like when consultants get close to their clients, they end up talking more, not less."

Questions for risk committees and CROs to consider:

- ? What techniques for driving board-management dialogue on risk has your risk committee or full board found particularly effective?
- ? How do you structure agendas and manage meetings so that policy approvals and regulatory requirements do not crowd out other key risk discussions?
- ? What is the right balance between presentation and discussion on risk matters? How do you create space for more open dialogue?
- ? How do you define success for the risk committee? On what performance metrics should the committee be evaluated?

3. Improving the board's level of understanding of the firm's risks

Board members must absorb and understand risk information for quality two-way dialogue to take place. Without sufficient knowledge of risk matters, participants note, committee meetings run the risk of devolving into a series of discussions focused on process and checklists.

One approach to increasing the board's knowledge level is, of course, changing the composition of the board itself, which has occurred at a number of banks since the financial crisis. Yet even with the changes in board membership, banks are still grappling with how best to build risk literacy within the board and key committees. Most CROs with whom we spoke agreed with the one who stated, *"We need a materially different understanding of risk [at the board level] … It can't mean directors simply become risk averse; it's about risk awareness."* Regulators are concerned too: one supervisor said, *"Directors need to get to the point where they have figured out what information they need and are not relying [solely] on management or the CRO."* Another regulator agreed: *"They need to do more than just consume [information]. They need to be able to develop a point of view in order to challenge management."* For their part, committee chairs say that there is a danger that board members may become overreliant on directors with deep experience in financial risk, with the result being *"a two-speed board."*

Directors and executives discussed the following challenges:

- Adapting the content and format of risk reports to increase their value to the board
- Maximising the value of director education sessions
- Ensuring non-committee members are included in knowledge-building efforts

Adapting the content and format of risk reports to increase their value to the board

For years, risk organisations have been experimenting with ways to, in words of the Basel Committee, "strike a balance between communicating information that is accurate and 'unfiltered' (i.e., that does not hide potentially bad news) and not communicating so much extraneous information that the sheer volume of information becomes counterproductive."[32] In early 2010, the Basel Committee's *Principles for Enhancing Corporate Governance* set forth a number of requirements for risk reporting to the board: risk reports should be "dynamic, comprehensive, and accurate … concise and meaningful … disaggregated … [but also] aggregated upward to allow for a firm-wide picture," and "clear about any deficiencies or limitations."[33]

No bank executive or board member would disagree with these principles, but they have many questions about how exactly to implement them. In the words of one CRO, *"What's the right level of information to provide? Do we give them everything, in the hope that they'll be able to synthesise it? Or do we do the synthesis? But then, it's [management's] synthesis."* A regulator commented, *"At every step, it becomes more difficult to ensure the information is complete and understandable … How can you make things easy to understand without leaving out the critical details?"* At the summit, a director noted, *"The challenge is to put the data and information into context."* In general, summit participants felt that risk reporting is still not sufficiently integrated, and furthermore, the data in many reports is not organised according to how frontline employees take and manage risks.

Research participants described widely varied approaches to board-level risk reporting. One CRO admitted, *"Our reports seem to be getting bigger all the time."* At another bank, *"[The risk report] was close to 200 pages. Now, the core [material] is 20–40 pages, with an appendix for reference."* At several banks reports tend to be 12–15 pages, with clusters of banks in the 30-page and 60-page ranges. Use of "supplementary detail" ranges from none at all to substantial appendices of 60 or more pages. The timing of reports varies as well, with some risk committees receiving reports only around scheduled meetings, while others receive regular updates outside of meetings as well. With board-level risk reporting still very much a work in progress, committees and boards are pushing management for improvements on a number of dimensions that they hope will make it easier for directors to absorb and comprehend complex risk issues:

- **More reader-friendly formats:** One risk committee member described management's reports as *"very elaborate – lots of league tables with information on exposures. I haven't yet seen a simple statement about our forward view on risk and how it fits with the bank's strategy."* A risk chair at another bank asked, *"Target credit [figures] and exposures: what is the committee supposed to do with that information? We get pages of numbers being presented to the board for approval."* A former risk executive advised CROs to put *"more emphasis on trends – the board needs numbers, but they also need to understand the story behind the numbers, and the patterns. Keep the numbers in the appendix and communicate in words and graphics."* At the summit, one director noted, *"I'm always looking for moves away from long-term trend data."*
- **More integrated, business-focused points of view:** At the summit a director observed, *"We have good communication on … risk by type, but probably too much segmentation. The risk committee must challenge that."* Said another, *"We need risk information organised according to the*

[32] Basel Committee on Banking Supervision, *Principles for Enhancing Corporate Governance*, page 21.
[33] Ibid.

way businesses actually operate." Some banks have used business-review reports to provide a most comprehensive, integrated picture of risks.

- **More decision-oriented analysis.** A director cautioned, *"We have all the arithmetic we need; it's the decisions that are the problem. I don't think it's worth spending time on [more or better metrics], instead, we should spend more time on what we're doing with them."* A fellow risk chair agreed: *"The committee is most interested in what's behind [the data] and what management proposes we do about it. Looking at our positions, what is easy or difficult to get out of? What's the price of taking our risk down in a certain area?"*
- **More transparent assumptions.** One participant commented, *"When I used to go to the board, I was always conscious of the multitude of assumptions that went into the risk reports … assumptions about normal distribution, about linkages and correlations between variables, and expectations about behaviour. So [CROs] have to share with the board what happens if our assumptions are wrong, and how much will it cost us?"*
- **A more journalistic approach to reports.** At one bank, the risk report is *"text heavy, with summaries at the top of each page … We don't use [slides]."* Some members of the risk organisation have taken writing courses in order to build skills in clear, concise prose communication and storytelling. According to the CRO, *"Some in management were taken aback, but sometimes people who really know the facts can't write, and vice versa."* Another bank has adopted a similar approach, making extensive use of headers, footers and callout text to ensure the risk report is easy to navigate and communicates key messages clearly.

Risk report components in use by banks

Most participants' reports include:

- Enterprise-wide dashboard
- Detail on individual risk areas: credit, market, liquidity, operational, etc.
- Metrics linked directly to the components of the risk appetite
- Qualitative assessment of changes in risk profile
- Stress scenarios and related analysis
- Updates by line of business and/or region
- External issues (e.g., regulatory trends, market conditions, current events)
- Risk mitigation actions and contingency plans

Several participants also cited:

- Balance sheet and P&L details
- Detailed "drill-downs" on specific risk categories or business unit risks
- In-depth analysis of investment portfolio
- Summaries of major news items (e.g., recent regulation)

Maximising the value of director education sessions

Participants agreed that, as one CRO put it, *"we need to accept that there will always need to be some education, and call it that. Otherwise [directors might] think, 'We're supposed to be educated now' … and feel more reluctant to ask questions."* Another participant commented that as with continuing education on accounting issues for audit committee members, *"we need to educate [risk committee members] and then verify. You can't just go to one course on risk and say that you're done."*

Boards and management are striving to develop ongoing risk education programmes that are substantive and tailored to individual director needs, as the Walker Report recommends.[34] Time constraints due to crowded committee agendas are one factor making this more difficult. Many risk committees find themselves in the situation described by one CRO: *"We're doing fewer education sessions and one-on-ones these days because there's simply no time."* One bank is incorporating webcasts on key topics into its director education programme as a way of giving time-pressed board members more opportunities to access education.

---

[34] David Walker, *A review of corporate governance in UK banks and other financial industry entities*, page 10.

Content is another challenge, as one participant noted: *"We've been asking the question, 'What's required for risk education?' The answer is inconvenient, because it's a lengthy one."* A number of external providers offer risk-focused education programmes or are in the process of designing them, but there are still fewer programmes available to risk committee members than are available to directors on audit committees.

Ensuring non-committee members are included in knowledge-building efforts

A number of research participants observed that at some banks, risk education and explication efforts tend to be primarily directed toward members of the risk committee – understandably so, since this group is likely to have the most urgent need for the greatest level of detailed knowledge. As a result, non-committee members may end up lagging behind in their understanding of key risk matters: *"The difference in knowledge [between the risk committee and the rest of the board] is big and will only get bigger over time,"* observed one CRO. Participants are taking several approaches to building up director knowledge outside the risk committee:

- **Open committee meetings or joint sessions:** Several banks issue standing invitations to all non-executive directors to attend risk committee meetings. One risk chair commented, *"Lately the entire board has been showing up for our committee meetings. Will they remain as enthusiastic over time? We'll see."* At one bank, all board members are on either the risk or the audit committee, and each board meeting includes a joint risk-audit meeting, so the full board hears about risk in two settings: at the committee level and the full board level. At the summit, a director noted that his risk committee now meets together with the audit committee for two hours at each scheduled board meeting.
- **Overlapping committee memberships:** Directors from a number of banks report their boards have some level of shared committee membership (mainly between the audit and risk committees, where these are separate), ranging from chairs only to several directors having overlapping membership.
- **Making time for risk education at full board meetings:** A director described how the risk chair at his bank requested that the CFO do a review of the bank's balance sheet at their most recent meeting of the full board: *"It gave directors an opportunity to ask basic educational questions which had not been aired previously. One great question was, 'If the bank wanted to decrease our balance sheet by half, how would [management] go about doing that?' We plan to do this review on an annual basis in the future."* A regulator commented, *"Periodically – at least annually – the CRO should be reporting to the full board."* Banks adopt different approaches to involving the CRO in boards meetings; in some, the CRO attends every meeting, in others, the CRO attends once a year or on an as-needed basis.

Practices for building risk literacy on the committee

- **Make use of active questioning.** One CRO described how he leads the risk committee through a debate on each issue: *"I ask them, 'Do you believe the leverage ratio should be X?' There's no right answer, but it starts the discussion. 'Now if I tell you our competitors look like Y, what would you say?' … If we are discussing emerging market risk, I ask them, 'What do you think the relative size of our emerging market risk should be? Would you have the same view if we have a [physical] presence in the country, versus if we are not in the country? … Do you think about our risk in area X as short term, or medium term?' If they say medium term, I ask them, 'What does that mean to you?' I don't want to talk at them; I want to bring them along, so they understand the different trade-offs inherent in risk areas."*

- **Devote time to "deep dives" on key topics.** Several banks report dedicating generous amounts of time, either within or outside of committee meetings, to focused discussions on risk topics. One bank holds sessions that are three to four hours in length between scheduled committee meetings, each devoted to a business area: *"The stated objective is to understand the risk and controls in each division, which really means, get to know the business."* At another bank, the deep dives focus on components of risk appetite; at a third, the CRO advises the committee chair on one or two current topics to cover in a 45-minute session, held once a quarter. Said one CRO, *"The issues will change, but over time, directors' knowledge will deepen."*

- **Dry-run the committee's questions for management.** The committee chair at one bank holds a pre-meeting with committee members to talk through not just the agenda, but the substance of meeting content, so that all directors feel able to engage and ask questions. *"This ensures directors come to the meeting as an informed committee, not as individuals with very different levels of understanding. We can spend time on discussion, not on having management report to us."*

- **Spend time outside the boardroom.** Each year, the committee at one bank spends several days in a different country, using that time to meet with management at key locations, get a feel for the local business climate and meet with regulators.

Clearly, raising the knowledge level of outside directors on complex, ever-evolving risk issues will be an ongoing, long-term effort. How can boards and committees gauge progress? According to one CRO, it is a good sign when *"[directors] are thinking about the connections between risks … At a recent meeting, when we walked them through the components [of risk appetite], they insisted on lowering the ROE [return on equity]. They said, 'There's no way you can hit this target if you hit all the others.'"* Another head of risk looks for meaningful exchanges on the content of management's proposals during committee meetings: *"When we bring material in, if it comes out at the end without any changes, how relevant was the discussion? Was it more of a face-saving exercise? Directors may have contributed and asked questions, but it's somewhat irrelevant if nothing changes."*

Questions for risk committees and CROs to consider:

- ? What is the board doing to ensure directors, and especially key committee members, sufficiently understand complex risk matters? How much knowledge is enough?
- ? What approaches have proven most effective for managing the volume, detail and utility of risk information provided to the board and to key committees? What types of information, either from within or outside the firm, would enable more robust board-management discussion on risk issues?
- ? What types of director education programmes, from which sources, are most effective in the area of risk? On which topics or issues, if any, are there unmet needs? How will you fill them?

4. Ensuring progress on risk governance is sustainable

For many banks, risk governance is a journey of continuous improvement – a "multiyear march," according to one respondent in the 2010 Ernst & Young global banking survey.[35] According to a number of research participants, that journey should include addressing the question of how to institutionalise the positive changes made to date, in order to reap the benefits over time. One supervisor described the steps banks have taken to improve board oversight of risks as *"very healthy and positive."* However, he went on to caution directors that *"when times are bad, everyone wants to be saved from too much risk. When times are good again, what will happen then? The key question for [bank boards and CROs] is the same as it is for regulators: can you take away the punch bowl while the party's still going on?"*

Participants highlighted several ways in which risk committees and CROs can consolidate and expand the progress their firms have made in risk governance since the crisis:

- Strengthen the profile of the risk organisation
- Improve the quality of risk data systems and infrastructure
- Ensure boards have access to a variety of external perspectives on risk

Strengthen the profile of the risk organisation

A summit participant observed that all too often, *"Risk officers were not, in fact, independent of the traders at the desk. They were more like advisers, but the traders' point of view prevailed.*" The chief risk officers with whom we spoke acknowledged that prior to the crisis, *"risk was not sufficiently well positioned to have a say,"* but express confidence that they possess the independence, access and authority needed to be heard and to make a difference when necessary. Indeed, according to a regulator, some banks even give their heads of risk a trading account to partially offset the risks in certain deals: *"It's rare, but it shows the CRO can get very actively involved."*

For their part, regulators say they plan to keep an open line of enquiry, through interviews with CROs and directors, to ensure CRO influence does not wane over time. One supervisor stated, *"The reporting*

[35] Ernst & Young, *Recover, adapt, advance: Back to business in an uncertain world,* page 11.

relationship is a cosmetic [thing] – the real question is, has the dynamic changed? To find this out, we need to talk to the participants. I can tell within five minutes – it's clear from the body language." Beyond qualitative assessments, supervisors say they will look for cases in which the CRO's authority has actually been exercised: *"Can [they] point me to deals that did not get done?"*

Participants called attention to two additional factors which could undermine the long-term success of the risk function:

- **Regulatory demands "crowding out" core activities.** Earlier this year, we reported that at some banks, regulatory matters now take up 40% of the risk organisation's time. At one organisation, the CRO is currently completing 19 separate surveys in response to regulatory requests; another CRO has identified over 200 best practices against which regulators are asking firms to benchmark themselves.[36] Responding to regulatory demands remains a challenge for risk functions: CROs at many banks are adding staff to try and keep up, but directors are concerned that *"[CROs] have been getting away from being real, independent advisers [due] to too much focus on regulatory change."*
- **Lack of bench strength.** One head of risk observed, *"There's a danger that the board puts too much focus on the CRO, to the exclusion of the broader team … If I were on the risk committee, I'd want to interview new senior hires in the risk organisation."* Another CRO described how *"in addition to bringing my executive team members to the risk committee, we also make sure [they] can spend some unstructured time with them outside meetings."* Several CROs said they aim to increase the rotations between the risk function and the businesses to build skills on both sides: *"It's a very good thing when firms make it clear you need x years in risk, and x years in the business in order to get to the top."* Participants note that assessing the risk team bench strength is critical, because CROs often have deep experience in some risk areas and less in others; looking for complementary skills in the broader team is thus important.

Improve the quality of risk data systems and infrastructure

At a gathering of non-executive directors earlier this year, Brian Peters, from the Federal Reserve of New York, recommended that boards "think about the quality of the infrastructure the firm needs to grow, especially IT. In banks, the front office always has the latest and greatest [systems], but the core infrastructure does not get the level of investment that is required."[37] CROs say that they are also eager to improve systems so that their teams can spend *"less time on scrubbing data and more time on analysis."*

According to the Ernst & Young risk survey of global banks, the improvements are well under way: 78% of respondents said they are in the process of upgrading technology and systems to support risk management, versus just 47% in 2009.[38] One CRO has created a new direct-report position with responsibility for data management and reporting, as well as other related activities such as modelling and stress testing. Still, many directors agree with one who acknowledged, *"I still worry that we get individual pieces [of data]; the hard*

---

[36] Ernst & Young and Tapestry Networks, "Risk governance in transition: the CRO perspective," 11 February 2010, page 2.
[37] Ernst & Young and Tapestry Networks, "Risk appetite, strategy, and regulatory reform," 16 June 2010, pp 8–9.
[38] Ernst & Young, *Recover, adapt, advance: Back to business in an uncertain world,* page 40.

part is to add it together." The director went on to say that although the bank might be comfortable with the data from five major areas of risk taken individually, the aggregated risk might be unacceptable.

Some industry participants point out that regulatory requirements have contributed to the problem: *"For Basel II, banks had built specific systems for regulatory reporting purposes, which are disconnected from our day-to-day risk management systems,"* commented a CRO. In addition, the expenditures on risk-reporting systems for regulators are, according to several CROs, squeezing budgets for much-needed risk-related infrastructure projects. Nuisance or not, regulatory demands in this area are here to stay. One supervisor declared that banks should expect *"regulators to be exponentially tougher on firms"* with respect to data and reporting in the future. For example, they will likely require more detailed reporting on a legal-entity basis and make additional data requests to feed into systemic risk analysis. *"Is this on banks' radar screens?"* asked this supervisor. *"I'm not sure they've thought through the implications."* Boards will need to keep pushing management to ensure adequate systems are in place to keep up with accelerating demands coming from both within and outside the firm.

Ensure boards have access to a variety of external perspectives on risk

A year ago, risk committee members and other board directors expressed interest in seeking independent views to complement the information received from management, but for many board members the idea still seemed relatively new.[39] In recent conversations, a number of industry participants have reported that their firms are bringing additional views on risk into the boardroom from a variety of sources:

- **Specialist advisers:** One board leader reported that the risk committee will be seeking external advice on *"specific issue[s]."* The advisers will be *"providing independent analysis and [offering] a general perspective on what others are doing and how we compare."* At another bank, directors came away from an engagement with an outside adviser *"with specific questions and next steps to follow up on. It was a refreshing perspective."*
- **The external audit firm:** A CRO commented, *"If I were a non-executive director, I'd insist on speaking with the external audit firm about risk … We can provide part of the education and information [for the committee], but we can't and shouldn't be all of it."* The European Commission's 2010 green paper on corporate governance raised the possibility of external auditors having a more formally defined role with respect to risk matters, asking "Should [external audit firms'] duty of information towards the board of directors and/or supervisory authorities on possible serious matters discovered in the performance of their duties be increased?"[40]
- **Analysts and investors:** One committee chair described how a discussion with activist investors about the bank's balance sheet raised a number of new questions that he subsequently took to management. Directors at a different bank are doing *"more talking with analysts who are covering [the institution]. Analysts are doing tons of research, all the time, and have useful perspectives."*

---

[39] Ernst & Young and Tapestry Networks, "Risk governance in a new era," *ViewPoints,* November 2009, page 13.

[40] European Commission, *Green paper: corporate governance in financial institutions and remuneration policies,* page 15.

- **Regulators:** Several summit participants said their boards regularly solicit views on risk matters from regulators both at home and, in some cases, in their firms' host countries. Others were wary about turning to regulators. One admitted that *"[regulators] do have a broad, cross-bank perspective,"* but another said, *"It is a [problem] if management or the board perceive the regulator as some kind of spy."*

While the external advisers to whom risk committees turn may vary, the common theme is that independent views on risk are an important way to keep discussions fresh and encourage an environment of constructive challenge.

Questions for risk committees and CROs to consider:

- ? What indicators does the board use to determine whether the CRO has the appropriate stature and independence within the firm? How can the risk committee gain insight into the bench strength and potential vulnerabilities of the risk organisation?
- ? How is the board working with the risk and IT functions to ensure the firm has the right systems and technology platforms to support risk governance today and into the future?
- ? How does the board ensure it receives independent perspectives on risks? Which sources have you found most and least useful in this regard? What additional information or sources would you like to incorporate into the board's risk discussions?

Conclusion

Risk governance is perhaps the best illustration of the central challenge bank boards face in the post-crisis environment: how to define the boundaries of active engagement such that directors do not cross the line into management's activities. It is by no means clear that detailed involvement is the answer: as one CRO observed, *"For so much of what went wrong in the crisis, knowing the deep detail would not have helped. The basic questions weren't being asked, [such as] 'Why are we making so much money in this business, and how does it compare to others?'"*

Boards and CROs are incorporating a number of approaches into their efforts to solving the risk governance challenge: grounding risk appetite firmly in the bank's strategy and statement of purpose, improving the quality of dialogue on risks, and sustaining hard-earned progress through investments in infrastructure, talent and information. Undoubtedly, each bank will make different choices on the priorities, pace, and scope of change depending on its culture and stage of the governance journey: as one CRO observed, *"It's easy to talk about the ideal risk committee, but we're all starting from very different places. And you need a clear vision of what you're looking to evolve into."* Regardless of their respective vantage points, research participants across sectors are aligned on the need and opportunity for progress. In the words of a summit participant, *"Never waste a crisis. This is a fantastic opportunity to accelerate change. If we play the old game a bit better, we're missing an opportunity. To what extent can we change the game?"*

Appendix 1: Research participants

Since early 2009, Tapestry Networks and Ernst & Young have been leading an initiative, the Bank Governance Leadership Network (BGLN), that brings together directors and executives from leading banks to discuss the board governance and risk oversight challenges confronting them and their institutions. In 2010, we conducted wide-ranging research into banks' risk governance practices and challenges, including extensive conversations with financial institution executives and board members, regulators and other thought leaders.

The list of participants includes:

Directors and executives

ABN AMRO Group NV

- Mr Hessel Lindenbergh, Supervisory Board Chairman

Bank of America

- Ms Susan Bies, Corporate Governance Committee Member, Enterprise Risk Committee Member
- Mr Donald Powell, Audit Committee Member, Compensation and Benefits Committee Member, Executive Committee Member

Bank of Montreal

- Ms Guylaine Saucier, Audit Committee Member, Risk Review Committee Member

Barclays PLC

- Sir Richard Broadbent, Deputy Chairman, Corporate Governance and Nominations Committee Member, HR and Remuneration Committee Chair
- Mr Hans-Joerg Rudloff, Chairman, Barclays Capital
- Sir John Sunderland, Corporate Governance and Nominations Committee Member, HR and Remuneration Committee Member

BNY Mellon

- Mr Nicholas Donofrio, Risk Committee Chair, Executive Committee Member
- Mr Brian Rogan, Chief Risk Officer

CIBC

- Ms Jalynn Bennett, Audit Committee Member
- Mr Gary Colter, Corporate Governance Committee Chair, Management Resources and Compensation Committee Member
- Mr Nicholas Le Pan, Risk Management Committee Chair, Corporate Governance Committee Member
- Mr Charles Sirois, Chairman
- Mr Tom Woods, Chief Risk Officer

Citigroup

- Mr. Michael E O'Neill, Risk Management and Finance Committee Member, Oversight Committee Chairman, Citi Holdings
- Mr Anthony Santomero, Risk Management and Finance Committee Member, Audit Committee Member
- Ms Diana Taylor, Personnel and Compensation Committee Member

Commerzbank

- Dr Bernd Voss, Advisory Board Member

Credit Suisse

- Mr Tobias Guldimann, Chief Risk Officer
- Mr Jean Lanier, Audit Committee Member
- Mr Anton van Rossum, Risk Committee Member

HSBC

- Mr John Coombe, Audit Committee Chair, Risk Committee Member, Remuneration Committee Member
- Mr Douglas Flint, Chief Financial Officer, Executive Director, Risk and Regulation
- Mr Brian Robertson, Chief Risk Officer

ICBC

- Sir Callum McCarthy, Strategy Committee Member, Risk Committee Member, and Nominations Committee Member

ING

- Mr Peter Elverding, Supervisory Board Chairman, Nomination Committee and Corporate Governance Committee Member, Remuneration Committee Member
- Mr Jackson Tai, Audit Committee Chair
- Mr Koos Timmermans, Chief Risk Officer

JPMorgan Chase

- Mr Laban Jackson, Jr, Audit Committee Chair
- Mr Barry Zubrow, Chief Risk Officer

Lloyds Banking Group

- Lord Alexander Leitch, Deputy Chairman, Audit Committee Member, HR and Remuneration Committee Member, Nominations and Governance Committee Member
- Ms Carol Sergeant, Chief Risk Officer

Macquarie Group

- Mr Stephen Allen, Chief Risk Officer
- Mr Michael Hawker, Risk Committee Member

Moody's Corporation/De Nederlandsche Bank

- Mr Ewald Kist, Board Member/Supervisory Board Member

Morgan Stanley

- Mr Roy Bostock, Nominating and Governance Committee Member
- Sir Howard Davies, Risk Committee Chair, Audit Committee Member
- Mr Kenneth deRegt, Chief Risk Officer
- Mr C Robert Kidder, Lead Director, Nominating and Governance Committee Member, Compensation, Management Development and Succession Committee Member
- Mr Donald Nicolaisen, Audit Committee Chair, Compensation, Management Development and Succession Committee Member

Nordea

- Ms Sarah Russell, Non-executive Director

Rabobank

- Mr Marinus Minderhoud, Audit, Compliance and Risk Committee Chair, Supervisory Board Member

RBC

- Mr Morten Friis, Chief Risk Officer

RBS

- Mr Nathan Bostock, Chief Risk Officer
- Sir Sandy Crombie, Senior Independent Director
- Sir Philip Hampton, Chairman
- Mr Arthur Ryan, Nominations Committee Member

Société Générale

- Mr Benoît Ottenwaelter, Chief Risk Officer
- Ms Nathalie Rachou, Audit and Risk Committee Member

Société Générale/UniCredit

- Mr Anthony Wyand, Vice President of the Board, Audit Committee Chair, Société Générale; Chairman, Internal Control and Risks Committee Chair, UniCredit

TD Bank

- Mr William Bennett, Audit Committee Chair, Risk Committee Member
- Mr Mark Chauvin, Chief Risk Officer
- Mr Brian Levitt, Corporate Governance Committee Member, Human Resources Committee Member
- Mr Harold MacKay, Risk Committee Chair, Audit Committee Member
- Mr John Thompson, Chairman, Corporate Governance Committee Chair, Human Resources Committee Member

UBS

- Mr Axel Lehmann, Risk Committee Member
- Mr Philip Lofts, Chief Risk Officer
- Mr William Parrett, Audit Committee Chair
- Mr David Sidwell, Risk Committee Chair, Strategy Committee Member

UniCredit

- Mr Karl Guha, Chief Risk Officer

U.S. Bancorp

- Ms Olivia Kirtley, Audit Committee Chair, Executive Committee Member, Governance Committee Member
- Mr Patrick Stokes, Risk Committee Chair, Executive Committee Member, Compensation and Human Resources Committee Member

Wells Fargo

- Ms Susan Engel, Credit Committee Member, Finance Committee Member, Human Resources Committee Member
- Mr Michael Loughlin, Executive Vice President and Chief Credit and Risk Officer
- Mr Philip Quigley, Lead Director, Governance and Nominating Committee Chair, Audit Committee Member

Westpac

- Mr John Curtis, Deputy Chairman, Audit Committee Member, Risk Management Committee Member, Remuneration Committee Member, Nominating Committee Member
- Mr Greg Targett, Chief Risk Officer

Zurich Financial Services

- Mr Tom de Swaan, Non-executive Director

Regulators and supervisors

- Mr Michael Alix, Senior Vice President, Bank Supervision Group, Federal Reserve Bank of New York
- Mr Frances Allen, Technical Specialist, Risk Framework & Capitals Unit, Prudential Risk Division, UK Financial Services Authority
- Mr Andrew Bailey, Executive Director, Banking, and Cashier, and Head of the Special Reasolution Units, Bank of England
- Mr Henk Brouwer, Executive Director, Banking Supervision and Supervisory Policy, De Nederlandsche Bank
- Mr Jean-Christophe Cabotte, Deputy Head of Division, Legal Analysis, French Banking Commission, Bank of France
- Mr Daryl Close, Associate – Risk, Special Projects, Risk Management Division, UK Financial Services Authority
- Ms Sally Dewar, Managing Director, Risk, UK Financial Services Authority
- Ms Kathryn Dick, Deputy Comptroller Credit and Market Risk, Office of the Comptroller of the Currency
- Mr Kyle Grieser, Chief of Staff, Senior Supervisors Group Secretariat, Federal Reserve Bank of New York
- Mr Thomas Huertas, Director, Banking Sector, UK Financial Services Authority
- Mr Fabrice Mace, Senior Adviser, French Banking Commission, Bank of France
- Mr Peter McCormack, Technical Specialist, Risk Framework & Capitals Unit, Prudential Risk Division, UK Financial Services Authority
- Mr Brian Peters, Senior Vice President, Federal Reserve Bank of New York
- Mr Ted Price, Assistant Superintendent, Supervision Sector, Office of the Superintendent of Financial Institutions
- Mr Richard Rosen, Senior Economist, Economic Advisor, Economic Research Department,
  Federal Reserve Bank of Chicago
- Mr William Rutledge, Executive Vice President, Bank Supervision Group, Federal Reserve Bank of New York
- Mr Carl Tannenbaum, Senior Vice President, Department of Supervision and Regulation, Federal Reserve Bank of Chicago

Ernst & Young

- Mr Andy Baldwin, Sub-Area Managing Partner, EMEIA Financial Services
- Mr Chris Bowles, Partner, UK Financial Services Risk Management Lead
- Mr Tom Campanile, Partner, Financial Services
- Dr Stephen Christie, Strategy and Business Incubation Lead
- Ms Martha Cook, Principal, Performance and Reward Practice
- Mr Peter Davis, Principal, Financial Services
- Mr Carmine DiSibio, Vice Chair and Managing Partner, Financial Services
- Mr Philippe D'Ornano, Enterprise Risk Services Leader, EMEIA
- Mr Mark Edelsten, Director, Performance and Reward Practice
- Mr Stephen Gregory, Partner, Advisory Services, EMEIA Financial Services
- Mr Chris Harner, Manager, Financial Services
- Ms Patricia Jackson, Head of Prudential Advisory Practice, EMEIA Financial Services

- Mr Dave Johnson, Partner, Human Capital Performance and Reward Practice
- Mr John Liver, Partner, Financial Services Advisory
- Mr Marcel van Loo, Banking and Capital Markets Leader, EMEIA Financial Services
- Mr John MacKay, Partner, Financial Services
- Mr Christopher Maher, Principal, Financial Services
- Mr Philip Middleton, Partner, Head of Financial Services Government, EMEIA Financial Services
- Ms Judy Modica, Senior Manager, Financial Services
- Ms Alexa Philo, Senior Manager, Financial Services
- Mr Lawrence Prybylski, Global Practices Leader, Financial Services Risk Management
- Mr William Schlich, Banking and Capital Markets Leader, Financial Services
- Mr Michael Schoonmaker, Principal, Performance and Reward Practice
- Mr Gary Stanton, Senior Manager, Regulatory Advisory, Team Leader, Wholesale and Investment Management
- Mr Donald Vangel, Advisor, Regulatory Affairs

About this document

The Bank Governance Leadership Network (BGLN) provides a unique forum in which key non-executive directors of major global banks can develop and share perspectives on the defining issues of the new banking environment, in conjunction with key internal and external constituencies. The network is convened by Tapestry Networks with the sponsorship and support of Ernst & Young.

ViewPoints aims to capture the essence of the BGLN discussion and associated research; it is produced by Tapestry Networks. Anyone who receives *ViewPoints* is encouraged to share it with those in their own network. The more board members, senior management, advisers, and stakeholders who become engaged in this dialogue, the more value will be created for all.